

A feature-augmented hybrid intrusion detection and prevention system for secure IoT networks

Vishal *

Department of Computer Applications

Lovely Professional University

Jalandhar 144411

Punjab

India

Ruchika Bhakhar [†]

Department of Computer Science and Engineering

School of Engineering & Technology

K. R. Mangalam University

Gurugram 122103

Haryana

India

Pallavi Pandey [§]

Department of Computer Science and Engineering

IILM University

Gurugram 122003

Haryana

India

Archana Goyal [‡]

Department of Computer Science and Engineering

School of Engineering and Technology

Noida International University

Greater Noida 203201

Uttar Pradesh

India

* E-mail: vishalhim@yahoo.com (Corresponding Author)

[†] E-mail: ruchika.bhakhar@krmangalam.edu.in

[§] E-mail: pallavi.pandey@iilm.edu

[‡] E-mail: archana.goyal@niu.edu.in

Manju Mandot [#]

*Department of Computer Science and Information Technology
Janardan Rai Nagar Rajasthan Vidyapeeth (Deemed-to-be University)
Udaipur 313001
Rajasthan
India*

Abstract

The rapid expansion of IoT devices has increased security risks due to limited resources, diverse protocols, and distributed environments. Traditional intrusion detection systems often fail to achieve high accuracy with low false alarms in such conditions. This study presents a Hybrid-IDPS that combines statistical traffic analysis with machine learning-based anomaly detection and feature enhancement. It integrates rule-based detection for known threats with a CNN and gradient boosting model for improved classification. A tiered edge-fog architecture enables real-time processing with low overhead. Experimental results show 98.7% accuracy and significantly reduced false positives, highlighting its efficiency and scalability for modern IoT applications.

Subject Classification: Primary 68M25, Secondary 68T27.

Keywords: IoT security, Intrusion detection, Hybrid-IDPS, Deep learning, Unsupervised clustering, Feature selection.

1. Introduction

The Internet of Things (IoT) [1], [2] is transforming modern society through the integration of smart sensors, embedded systems, and communication technologies, enabling automated and data-driven environments across domains such as healthcare, smart cities, education, and digital platforms. However, this rapid growth has also increased exposure to cyber threats within heterogeneous device ecosystems. IoT networks pose unique security challenges, including limited computational resources, diverse communication protocols, high data volumes, and weak device-level protection, making traditional security solutions less effective [3], [4].

Intrusion Detection and Prevention Systems (IDPS) are essential for safeguarding IoT environments, yet existing approaches have limitations. Signature-based methods [5]-[8] are effective for known threats but fail against new attacks, while anomaly-based techniques [9], [10] can detect unknown patterns but often produce high false positives. Even advanced systems face issues of scalability, adaptability, and real-time performance in IoT contexts [11], [12].

To address these gaps, this study proposes a Hybrid-IDPS that integrates supervised clustering with unsupervised K-Means clustering to enhance

[#] E-mail: manju.mandot@gmail.com

detection accuracy. Cluster labels are used as augmented features for a neural classifier.

2. Literature Review

The security of IoT networks has been widely explored using diverse intrusion detection strategies. Signature-based approaches [1], [2] remain effective for identifying known attack patterns with low false-positive rates; however, their dependence on predefined signatures limits their ability to detect emerging threats. In contrast, anomaly-based detection methods [3], [4] model normal network behavior and identify deviations, enabling detection of unknown attacks, though they often suffer from high false alarms and sensitivity to dynamic traffic conditions.

Recent advancements emphasize machine learning and deep learning techniques for improved intrusion detection. Neural network-based and deep learning approaches [5], [6] have demonstrated enhanced capability in capturing complex and nonlinear attack patterns in IoT environments. Despite their effectiveness, these methods typically require high computational resources and large labeled datasets, which restrict their deployment in resource-constrained scenarios.

Clustering techniques, particularly K-Means [7], have been utilized to uncover hidden traffic structures and support unsupervised learning in intrusion detection. Additionally, feature selection methods such as Random Forest [8] help identify the most relevant attributes, improving classification accuracy while reducing computational overhead. Emerging studies [9]-[11] further highlight the importance of advanced feature engineering, blockchain-based security frameworks, and IoT analytics in strengthening cyber defense mechanisms. Mathematical modeling techniques [12] also contribute to optimizing system performance.

Although significant progress has been made, existing solutions often rely on isolated learning paradigms. The lack of integration between supervised and unsupervised methods, along with limited use of feature augmentation, motivates the development of more adaptive and scalable hybrid intrusion detection frameworks for IoT security.

3. Proposed Hybrid-IDPS Framework

The proposed Hybrid Intrusion Detection and Prevention System (Hybrid-IDPS) address key challenges in IoT networks by integrating multiple analytical techniques, including deep neural architecture and unsupervised clustering, within a layered framework as being shown in the given Figure 1.

techniques, including deep neural architecture and unsupervised clustering, within a layered framework as being shown in the given Figure 1.

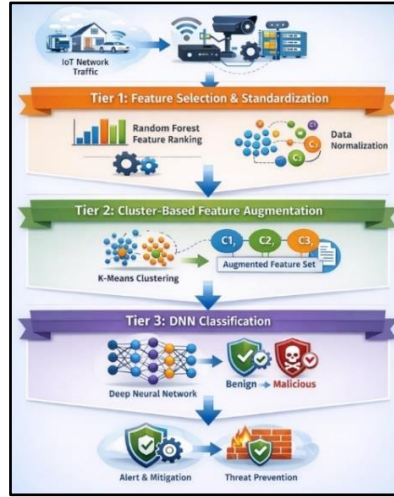


Figure 1
Three-Tier Architecture of the Proposed Hybrid-IDPS for IoT Networks.

3.1 Feature Selection and Data Standardization

The proposed framework is illustrated in Figure 1, preprocesses IoT traffic using normalization and Random Forest-based feature ranking. K-Means Clustering augments features, while a Deep Neural Network classifies threats, enabling real-time detection, alerting, and efficient security management in IoT environments. Algorithm 1 is given for the Feature Selection and Data Standardization.

3.1.A. Input Dataset Representation

Let the raw IoT traffic dataset be:

$$\mathcal{D} = \{(\mathbf{x}_i, y_i)\}_{i=1}^N$$

3.1.B. Data Standardization (Z-score Normalization)

Each feature x_j is standardized to have zero mean and unit variance:

$$x'_{ij} = \frac{x_{ij} - \mu_j}{\sigma_j}$$

where:

- $\mu_j = \frac{1}{N} \sum_{i=1}^N x_{ij}$ is the mean of the feature j ,
- $\sigma_j = \sqrt{\frac{1}{N} \sum_{i=1}^N (x_{ij} - \mu_j)^2}$ is the standard deviation of the feature j ,
- x'_{ij} is the standardized value.

The standardized dataset becomes:

$$\mathcal{D}' = \{(\mathbf{x}'_i, y_i)\}_{i=1}^N$$

Algorithm 1: Feature Selection and Data Standardization

Algorithm 1: Feature Selection and Data Standardization

Input: Raw dataset $\mathcal{D} = \{(\mathbf{x}_i, y_i)\}_{i=1}^N$, number of trees T , selected feature count K

Output: Reduced standardized dataset $\mathcal{D}_{sel}$

```

1: Input: Raw dataset  $\mathcal{D} = \{(\mathbf{x}_i, y_i)\}_{i=1}^N$ 
2: Initialize standardized dataset  $\mathcal{D}'$ 
3: for each feature  $j = 1$  to  $d$  do
4:   Compute mean  $\mu_j$  and standard deviation  $\sigma_j$ 
5:   for each sample  $i = 1$  to  $N$  do
6:      $x'_{ij} = (x_{ij} - \mu_j) / \sigma_j$ 
7:   end for
8: end for
9:  $\mathcal{D}' \leftarrow \{(\mathbf{x}'_i, y_i)\}$ 
10: Train Random Forest model  $F_{RF}$  with  $T$  trees on  $\mathcal{D}'$ 
11: for each feature  $j = 1$  to  $d$  do
12:    $\text{Imp}(j) \leftarrow 0$ 
13:   for each tree  $k = 1$  to  $T$  do
14:     Compute impurity reduction  $\Delta I_{jk}$ 
15:      $\text{Imp}(j) \leftarrow \text{Imp}(j) + \Delta I_{jk}$ 
16:   end for
17:    $\text{Imp}(j) \leftarrow \text{Imp}(j) / T$ 
18: end for
19: Rank all features in descending order of  $\text{Imp}(j)$ 
20: Select top- $K$  features  $\rightarrow F_{sel}$ 
21: for each sample  $i = 1$  to  $N$  do
22:    $\mathbf{z}_i \leftarrow$  extract features from  $\mathbf{x}'_i$  using  $F_{sel}$ 
23: end for
24:  $\mathcal{D}_{sel} \leftarrow \{(\mathbf{z}_i, y_i)\}$ 
25: Return  $\mathcal{D}_{sel}$ 

```

3.2 Cluster-Based Feature Augmentation

K-Means clustering is applied to reduced features to identify hidden traffic patterns. Generated cluster labels are appended as new features, enriching context and improving differentiation between normal and malicious network behavior.

3.2.A. Mathematical Formulation

1. Input Representation

Let the reduced standardized dataset from Stage 1 be:

$$\mathcal{D}_{sel} = \{(\mathbf{z}_i, y_i)\}_{i=1}^N, \mathbf{z}_i \in \mathbb{R}^K$$

where:

- N = number of samples,
- K = number of selected features,
- $\mathbf{z}_i = [z_{i1}, z_{i2}, \dots, z_{iK}]$ = reduced feature vector,
- y_i = class label (used later for supervised classification only).

3.2. B. K-Means Objective Function

The goal of K-Means is to partition the dataset into C clusters by minimizing the within-cluster sum of squared distances (WCSS):

$$\mathcal{J} = \sum_{c=1}^C \sum_{\mathbf{z}_i \in \mathcal{C}_c} \|\mathbf{z}_i - \boldsymbol{\mu}_c\|^2$$

where:

- C = number of clusters,
- $\mathcal{C}_c$ = set of points assigned to cluster c ,
- $\boldsymbol{\mu}_c \in \mathbb{R}^K$ = centroid of cluster c ,
- $\|\cdot\|$ = Euclidean norm.

3.2.C. Initialization of Centroids

Centroids are initialized randomly or via K-Means++:

$$\boldsymbol{\mu}_c^{(0)} \sim \text{Uniform}(\mathcal{D}_{sel}), c = 1, 2, \dots, C$$

3.2.D. Assignment Step (E-Step)

Each data point $\mathbf{z}_i$ is assigned to the nearest centroid based on Euclidean distance:

$$\ell_i^{(t)} = \arg \min_{c \in \{1, \dots, C\}} \|\mathbf{z}_i - \boldsymbol{\mu}_c^{(t)}\|^2$$

where:

- $\ell_i^{(t)}$ = cluster label for sample i at iteration t ,
- $\boldsymbol{\mu}_c^{(t)}$ = centroid of cluster c at iteration t .

3.3. Derivation of the Centroid Update Rule

To minimize the objective function $\mathcal{J}$ with respect to $\boldsymbol{\mu}_c$, take the partial derivative:

$$\mathcal{J}_c = \sum_{\mathbf{z}_i \in \mathcal{C}_c} \|\mathbf{z}_i - \boldsymbol{\mu}_c\|^2$$

Expand the squared norm:

$$\mathcal{J}_c = \sum_{\mathbf{z}_i \in \mathcal{C}_c} (\mathbf{z}_i - \boldsymbol{\mu}_c)^T (\mathbf{z}_i - \boldsymbol{\mu}_c)$$

Differentiate w.r.t. $\boldsymbol{\mu}_c$:

$$\frac{\partial \mathcal{J}_c}{\partial \boldsymbol{\mu}_c} = \sum_{\mathbf{z}_i \in \mathcal{C}_c} 2(\boldsymbol{\mu}_c - \mathbf{z}_i)$$

Set derivative to zero:

$$\begin{aligned} \sum_{\mathbf{z}_i \in \mathcal{C}_c} (\boldsymbol{\mu}_c - \mathbf{z}_i) &= 0 \\ |\mathcal{C}_c| \boldsymbol{\mu}_c - \sum_{\mathbf{z}_i \in \mathcal{C}_c} \mathbf{z}_i &= 0 \\ \Rightarrow \boldsymbol{\mu}_c &= \frac{1}{|\mathcal{C}_c|} \sum_{\mathbf{z}_i \in \mathcal{C}_c} \mathbf{z}_i \end{aligned}$$

This confirms that the centroid update rule is the arithmetic mean of all points in the cluster c .

3.4. DNN-Based Classification

The final stage utilizes a Deep Neural Network (DNN) to classify augmented traffic features as benign or malicious. It captures complex nonlinear relationships within the enriched feature space, enabling accurate decision-making. The model is optimized for efficiency, balancing detection performance and computational requirements, making it suitable for real-time IoT deployment.

3.4.A. Mathematical Formulation

3.4.B. Input Representation

Let the augmented dataset from Stage 2 be:

$$\tilde{\mathcal{D}} = \{(\tilde{\mathbf{z}}_i, y_i)\}_{i=1}^N, \tilde{\mathbf{z}}_i \in \mathbb{R}^M$$

where:

- $M = K + 1$ (or $K + C$ for one-hot cluster encoding),
- $y_i \in \{0, 1\}$ (0: benign, 1: malicious).

4. Experimental Results and Discussions.

This section presents the experimental evaluation of the proposed Hybrid-IDPS framework using benchmark datasets (CICIDS2018 and CSEIC-IDS2018). The framework is assessed against baseline intrusion detection models, including a standalone DNN, a KMeans+SVM hybrid model, and a Random Forest-based IDS. Performance is analyzed using standard classification metrics and system-level resource utilization indicators to validate both detection effectiveness and deployment feasibility in IoT environments.

4.1 Detection Performance Analysis

Table 1 summarizes the classification performance of all compared models. The proposed Hybrid-IDPS achieves the highest accuracy of 98.7%,

outperforming the DNN-only and clustering-based baselines. It also demonstrates superior precision (98.4%) and recall (98.9%), indicating a strong ability to correctly identify both benign and malicious traffic flows. Notably, the false positive rate is reduced to 1.3%, which is critical for minimizing unnecessary alerts and operational overhead in real-world IoT deployments.

Table 1
Comparison of Detection Performance Across IDS Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
Proposed Hybrid-IDPS	98.7	98.4	98.9	98.6	1.3
DNN-Only	94.2	93.1	95	94	4.8
KMeans+SVM	90.5	89.7	90.2	89.9	7.6
Random Forest IDS	92.8	91.9	93.5	92.7	5.4

The performance gains validate the effectiveness of cluster-based feature augmentation and ensemble-driven feature selection in enhancing discrimination between benign and malicious traffic patterns.

5. Conclusion

This study presents a Hybrid Intrusion Detection and Prevention System (Hybrid-IDPS) for IoT security, integrating ensemble-based feature selection, clustering-based feature enhancement, and deep neural network classification within a layered architecture. By combining Random Forest-based feature importance with supervised and unsupervised K-Means clustering, the model captures both explicit and hidden traffic patterns, improving detection capability. Evaluation on CICIDS2018 and CSECIC-IDS2018 datasets shows superior performance, achieving 98.7% accuracy and significantly reducing false positives. The framework also demonstrates low computational overhead, making it suitable for constrained environments. Future work includes multi-class classification, incremental learning, and federated approaches for enhanced scalability.

References

[1] B. Nawaal, U. Haider, I. U. Khan, and M. Fayaz, "Signature-based intrusion detection system for IoT," in *Cyber Security for Next-Generation Computing Technologies*. Boca Raton, FL, USA: CRC Press, pp. 141–158 (2024), doi: 10.1201/9781003404361-8.

- [2] M. Agoramoorthy, A. Ali, D. Sujatha, M. Raj T. F., and G. Ramesh, "An analysis of signature-based components in hybrid intrusion detection systems," in *Proc. 2023 Intell. Comput. Control Eng. Bus. Syst. (ICCEBS)*, pp. 1–5 (2023), doi: 10.1109/ICCEBS58601.2023.10449209.
- [3] M. Bhavsar, K. Roy, J. Kelly, and O. Olusola, "Anomaly-based intrusion detection system for IoT application," *Discov. Internet Things*, vol. 3, no. 1, Art. no. 5 (2023), doi: 10.1007/s43926-023-00034-5.
- [4] S. Bacha, A. Aljuhani, K. B. Abdellafou, O. Taouali, N. Liouane, and M. Alazab, "Anomaly-based intrusion detection system in IoT using kernel extreme learning machine," *J. Ambient Intell. Humaniz. Comput.*, vol. 15, no. 1, pp. 231–242 (2024), doi: 10.1007/s12652-022-03887-w.
- [5] M. Schrötter, A. Niemann, and B. Schnor, "A comparison of neural-network-based intrusion detection against signature-based detection in IoT networks," *Information*, vol. 15, no. 3, Art. no. 164 (2024), doi: 10.3390/info15030164.
- [6] M. A. Alsoufi, M. M. Siraj, F. A. Ghaleb, M. Al-Razgan, M. S. Al-Asaly, T. Alfakih, and F. Saeed, "Anomaly-based intrusion detection model using deep learning for IoT networks," *Comput. Model. Eng. Sci.*, vol. 141, no. 1, Art. no. 1 (2024), doi: 10.32604/cmesci.2024.052112.
- [7] Y. Peng, K. Li, and M. Li, "A novel K-means clustering algorithm and its application," *J. Comput. Theor. Nanosci.*, vol. 12, no. 10, pp. 3658–3661 (2015), doi: 10.1166/jctn.2015.4253.
- [8] G. Biau and E. Scornet, "A random forest guided tour," *TEST*, vol. 25, pp. 197–227 (2016).
- [9] B. L. V. S. Aditya and S. N. Mohanty, "Design of an efficient model for fake profile detection on social media using advanced feature engineering and deep learning techniques," *J. Inf. Optim. Sci.*, vol. 46, no. 6, pp. 1803–1810 (2025), doi: 10.47974/JIOS-2009.
- [10] S. D. Bahinipati and B. K. Pattanayak, "A novel blockchain-enabled smart contract for smart city e-governance ecosystem," *J. Inf. Optim. Sci.*, vol. 46, no. 6, pp. 1831–1840 (2025), doi: 10.47974/JIOS-2012.

- [11] Z. S. Alsham, E. Bahçekapılı, and A. Ayaz, "Trends in IoT applications in smart campuses: A topic modeling approach," *COLLNET J. Scientometrics Inf. Manag.*, vol. 19, no. 1, pp. 21–40 (2025), doi: 10.47974/CJSIM-2024-017.
- [12] W. Sripanya, W. Rungrottheera, and H. Park, "Fourier series analysis and computation based on function characteristics," *J. Interdiscip. Math.*, vol. 28, no. 6, pp. 2109–2120 (2025), doi: 10.47974/JIM-2352.

Received December, 2025